Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

European national news☆

Mark Turner

Herbert Smith Freehills LLP, London, United Kingdom

Keywords:
Internet
ISP/Internet service provider
Software
Data protection
IT/Information technology
Communications
European law/Europe

ABSTRACT

The regular article tracking developments at the national level in key European countries in the area of IT and communications – co-ordinated by Herbert Smith LLP and contributed to by firms across Europe. This column provides a concise alerting service of important national developments in key European countries. Part of its purpose is to compliment the Journal's feature articles and briefing notes by keeping readers abreast of what is currently happening "on the ground" at a national level in implementing EU level legislation and international conventions and treaties. Where an item of European National News is of particular significance, CLSR may also cover it in more detail in the current or a subsequent edition.

1. Belgium

1.1. *Belgian court of cassation confirms that ISPs can be requested to block all domain names leading to certain websites*

The Belgian Court of Cassation recently upheld an order by an investigative judge to block all domain names leading to the file sharing website, "The Pirate Bay".

In April 2012, an investigative judge issued an order to Telenet, a Belgian Internet Service Provider (the "ISP") to block all domain names leading to the servers of The Pirate Bay. Consequently, the ISP contested this order in court seeking rescission of the order for lack of legal grounds, and failing that to obtain more clarity on the contents of the order and how to comply with it.

The petition of the ISP was dismissed twice by the lower courts, so the ISP turned to the Court of Cassation. In its judgment of 22 October 2013, the Court of Cassation confirmed the decisions of the lower courts.

The ISP had initially argued that Articles 35 to 39bis of the Code of Criminal Procedure ("CCP") only envisages fact-finding, and was not intended to prevent further perpetrations of such alleged infringements. The Court dismissed this argument stating that the Articles cited can be used not only for fact-finding, but also to stop certain acts which appear to constitute a criminal offence, or to protect civil interests.

The ISP further argued that Article 39bis CCP was directed to those who store or allow data to be stored, and not at those who merely provide access to the communication network and who have no power to control or dispose of this data. Likewise, the ISP argued that an order based on Article 39bis CCP should only aim to seal the IT system in order to safeguard the integrity of the data, and that this is impossible in this case, as the operators of The Pirate Bay can still gain access to their servers. The Court rejected this argument.

Lastly, the ISP also cited the E-commerce Act and the prohibition contained therein to impose a general monitoring obligation. The ISP argued that the order does not specify the means that it should use to comply with the obligation imposed on them. Furthermore, it does not exhaustively list

☆ **Mark Turner** (mark.turner@hsf.com) Partner, Herbert Smith Freehills LLP and member of the CLSR Professional Board, and **Edward du Boulay**, Associate (edward.duboulay@hsf.com) (Tel.: +44 20 7374 8000). For further information about Herbert Smith Freehills LLP see: www.herbertsmithfreehills.com.

0267-3649/$ – see front matter
http://dx.doi.org/10.1016/j.clsr.2013.12.007

the domain names which should be blocked, nor does it contain a time limit. The ISP therefore asked the Court to refer several questions to the European Court of Justice, in order to determine whether the order was compatible with EU legislation.

The Court refused this request and declared that the order given to an ISP to block, by all technical means, all domain names that refer to The Pirate Bay domain name, did not constitute a general monitoring obligation. The Court did not elaborate on the grounds for this decision.

***Cédric Lindenmann**, Associate (cedric.lindenmann@stibbe.com) and **Laura Verhoeven**, Trainee (laura.verhoeven@stibbe.com) from Stibbe, Brussels (Tel.: +32 2 533 53 51).*

2. Denmark

2.1. *Digitally signed loan documents held to be unenforceable*

A new ruling from the Danish Western High Court states that digitally signed loan agreements are not directly enforceable at the Enforcement Courts. Banks and other creditors therefore still need to obtain a physical signature from the debtor in order to make the loan document directly enforceable at the Enforcement Courts.

Physically signed loan agreements are directly enforceable at the Enforcement Courts in accordance with the Danish Administration of Justice Act. The Administration of Justice Act does not mention the matter of enforceability of digitally signed loan agreements, and the Western High Court has now ruled that these documents are not covered by the Act.

As a consequence the debt on a digitally signed loan document cannot be recovered directly through the Enforcement Courts in the event of the debtor's default on payment, even though the loan agreement specifically includes an enforceability clause.

The ruling, however, has no effect on the validity of the loan agreement; the debtor is still bound by the stipulations of the agreement and is obliged to pay the agreed instalments and interest.

Banks and other creditors who have loan documents digitally signed by debtors will have to obtain a physical signature from the debtor in order to make it directly enforceable. In case the debtor does not wish to sign the document physically, the creditors will have to go through the regular court system to get an execution judgment, or file a small-money claim form at the Enforcement Court if the owed amount does not exceed the statutory threshold.

2.2. *Legislative work in progress*

The Department of Justice is currently working on a revision of the Administration of Justice Act. A working group has been assigned to research possible amendments to the rules on enforceability, including the enforceability of digitally signed documents. A conclusion of the legislative work and a revised Act is expected in the summer of 2014. It is expected that the amended Act will contain provisions making digitally signed document directly enforceable.

***Carsten Raasteen**, Partner, cr@kromannreumert.com and **Julie Aaby Ryttov**, Assistant Attorney, jry@kromannreumert.com from Kromann Reumert, Copenhagen office, Denmark (Tel.: +45 70 12 12 11).*

3. France

No contribution for this issue.

***Alexandra Neri**, Partner, alexandra.neri@hsf.com and **Jean-Baptiste Thomas-Sertillanges**, Avocat, Jean-Baptiste.Thomas-Sertillanges@hsf.com, from the Paris Office of Herbert Smith Freehills LLP (Tel.: +33 1 53 57 78 57).*

4. Germany

4.1. *Facebook and data protection*

Facebook Inc. recently won a high-profile data protection case before a German court. It was held that the German data protection laws, which are known for providing a comparatively high standard of security, are not applicable in the case of services that Facebook provides in Germany (OVG Schleswig-Holstein, 4 MB 11/13).

In its judgment, the highest administrative court of the State of Schleswig-Holstein had to decide whether section 1(5) of the German Data Protection Act (BDSG) should be interpreted widely or narrowly. The provision states that German data protection law should be applicable if a foreign entity is collecting, processing or using personal data in Germany. However, there is an exception: if a data controller collects, processes, or uses personal data in Germany but is actually located in another member state of the EU or the EEA, German data protection law does not apply. If this foreign entity uses a German branch to do the processing, however, then this exception in turn does not apply.

The California-based Facebook Inc. has a branch in Ireland, Facebook Ireland Ltd., and a branch in Germany, Facebook Germany GmbH. The Court held that since Facebook Germany GmbH was only concerned with marketing and acquisition of advertisements it did not qualify as a relevant branch in the sense of sect. 1(5) BDSG. Instead, the Court regarded Facebook Ireland Ltd. as the branch which collects, processes and uses the contact information of registered users, since it operated with a staff of 400 people through "stable arrangements" and thus fulfilled the requirements of a branch under Recital 19 of the Data Protection Directive 95/46/EG. Therefore, the Court held that this scenario is, in fact, a case of the exception, in which the entity that collects, processes, or uses personal data in Germany is actually located in another member state of the EU, without using a German branch.

We note that the application and interpretation of national data protection laws may change if the proposed General Data Protection Regulation is enacted which is anticipated to create a fully harmonized European standard of data protection.

***Dr Stefan Weidert**, LL.M. (Cornell), Partner (stefan.weidert@gleisslutz.com), of the Berlin Office of Gleiss Lutz, Germany (Tel.: +49 30 800 979 0).*